Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of managing security keys provided to users of a service, the method comprising the steps of:

issuing a security key to a first user eligible to receive the service;

monitoring the first user's status to establish whether the first user is eligible to receive the service;

establishing, in accordance with a policy, a first value associated with invalidation of the first user's security key at a particular point in time, and a second value associated with providing the service to an ineligible user at the particular point in time, and if the second value exceeds the first value, invalidating the first user's security key at the particular point in time,

wherein the first user's security key is kept valid if the second valid does not exceed the first value, and

wherein the policy provides that the second value is related to the economic penalty associated with provision of the service to the ineligible user.

2. (Currently Amended) A method according to claim 1 wherein the policy further provides that the first value is related to the economic penalty associated with reconfiguration of security keys issued to other users consequent to invalidation of the first user's security key.

3. (Canceled).

4. (Currently Amended) A method according to claim [[3]] 1 wherein the second value is calculated by aggregating the economic penalty associated with provision of the service to each ineligible user.

5. (Original) A method according to claim 4 wherein the economic penalty associated with provision of service to ineligible users includes a value representative of dilution of economic value to eligible users consequent to provision of the service to ineligible users.

6. (Currently Amended) A method according to claim [[3]] 1 wherein the economic penalty of providing the service to ineligible users includes any costs arising from the provision of network and server capacity to ineligible users.

7. (Currently Amended) A method according to claim 2 wherein the security keys are generated in an ancestrally-based hierarchy, and wherein invalidation of a given key necessitates a need for reconfiguration of each security key in the hierarchy.

8. (Currently Amended) A method according to claim 7 wherein upon invalidation of a given security key, an other security key requires reconfiguration only to the extent that it shares common ancestor security keys with the given invalidated security key.

9. (Original) A method according to claim 8 wherein the hierarchy is a binary tree.

10. (Currently Amended) A method of managing provision of security keys to a plurality of users of a network service, the method comprising the steps of:

generating plurality of security keys, each of which is related ancestrally to at least one other security key of the plurality of security keys;

issuing security keys to users;

monitoring users' status [[to]] for continuing eligibility for consumption of the service; and

upon establishing ineligibility of a user, determining upon the basis of a predetermined policy, a value for economic disbenefit to a provider of the service of (a) invalidation of the ineligible user's security key; and (b) provision of service to an ineligible user.

11. (Currently Amended) A method according to claim 10 further comprising the step of invalidating the security key if the disbenefit of providing service to an ineligible user is greater than the disbenefit of invalidating the security key.

12. (Currently Amended) A method according to claim 11 further comprising the step of aggregating the disbenefit of providing the service to each ineligible user, and invalidating the security key only if the aggregated disbenefit of providing the service to all ineligible users is greater than the disbenefit of invalidating the security key.

13. (Currently Amended) A method according to claim 10 wherein invalidation of the security key necessitates reconfiguration of each other security key to the extent another security key shares common ancestry with the invalidated security key.

14. (New) A method according to claim 9, further comprising the step of:

assigning security keys to users based on a length of time subscribed to for the service,

wherein a first set of users who have subscribed for a length of time less than a predetermined time are assigned security keys in a first subsection of the binary tree,

wherein a second set of users who have subscribed for a length of time greater than or equal to the predetermined time are assigned security keys in a second subsection of the binary tree, and

wherein the security keys of the first subsection of the binary tree only share a first generation root key as a common ancestor with the security keys of the second subsection of the binary tree.

15. (New) A method according to claim 13, wherein the related ancestry of the security keys is determined by way of a binary tree in which the security keys are assigned,

wherein the issuing step comprising the step of:

assigning security keys to the users based on a length of time subscribed to for the service,

wherein a first set of users who have subscribed for a length of time less than a predetermined time are assigned security keys in a first subsection of the binary tree,

wherein a second set of users who have subscribed for a length of time greater than or equal to the predetermined time are assigned security keys in a second subsection of the binary tree, and

wherein the security keys of the first subsection of the binary tree only share a first generation root key as a common ancestor with the security keys of the second subsection of the binary tree.

16. (New) A method according to claim 4, wherein the security keys are generated in an ancestry-based, binary tree hierarchy,

wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy,

wherein the first value is computed by adding a first cost associated with invalidating all security keys of the ineligible users, with a second cost associated with reconfiguring all security keys of eligible users that are in an ancestry chain of any one of the security keys of the ineligible users.

17. (New) A method according to claim 10, wherein the security keys are generated in an ancestry-based, binary tree hierarchy,

wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy,

wherein the value for economic disbenefit to the provider is computed by adding a first cost associated with invalidating the ineligible user's security key, with a second cost associated with reconfiguring all security keys of eligible users that are in an upper ancestry level in a same ancestry chain as the ineligible user's security key, and with a third cost associated with invalidating all security keys in the binary tree hierarchy that are of a lower ancestry level in the same ancestry chain as the ineligible user's security key.

18. (New) A method according to claim 1, wherein the issuing step is performed by a server, and wherein the issuing step includes providing the security key to the first user in a cookie returned to the first user by the server over the Internet.

19. (New) A method according to claim 10, wherein the issuing step is performed by a server, and wherein the issuing step includes providing the security keys to the users in cookies respectively returned to the users by the server over the Internet.

20. (New) A method according to claim 17, wherein the second cost includes a cost associated with creating a new binary tree to provide a new set of security keys to replace all invalidated security keys.

21. (New) A method according to claim 18, wherein the third cost includes a cost associated with creating a new binary tree to provide a new set of security keys to replace all invalidated security keys.